CLAIMS:

1. A method for selectively activating biometric sensors (102, 104, 106) to authenticate the identity of an individual while conserving system resources, comprising the acts of:

activating a first tier biometric sensor (102) to verify the biometric of said individual; and

activating a second tier biometric sensor (104, 106) to verify the biometric of said individual in the case where said individual is successfully verified with said first tier biometric sensor (102).

2. The method of Claim 1, wherein said second tier biometric sensor (104, 106) is a comparatively more sophisticated sensor than said first tier biometric sensor (102).

3. A method for selectively activating biometric sensors (102, 104, 106) to authenticate the identity of an individual while conserving system resources, comprising the acts of:

activating a first tier biometric sensor (102) to verify the biometric of said individual; and

activating a second tier biometric sensor (104, 106) to verify the biometric of said individual in the case where said individual is unsuccessfully verified with said first tier biometric sensor (102).

4. The method of Claim 3, wherein said second tier biometric sensor (104, 106) is a comparatively more sophisticated sensor than said first tier biometric sensor (102).

5. A method for selectively activating biometric sensors (102, 104, 106) to authenticate the identity of an individual while conserving system resources, comprising the acts of:

activating a first tier biometric sensor (102) to verify the biometric of said individual;

determining whether said individual desires a service level exceeding a predetermined service level threshold; and

activating a second tier biometric sensor (104, 106) to verify the biometric of said individual when it determined that said individual desires said service level exceeding said threshold.

6. The method of Claim 5, wherein said second tier biometric sensor (104, 106) is a comparatively more sophisticated sensor than said first tier biometric sensor (102).

7. A method for selectively activating biometric sensors (102, 104, 106) to authenticate the identity of an individual while conserving system resources, comprising the acts of:

activating a first tier biometric sensor (102) to verify the biometric of said individual;

determining whether an environmental parameter is outside of a predetermined range; and

activating a second tier biometric sensor (104, 106) to verify the biometric of said individual when said environmental parameter is determined to be outside said predetermined range.

8. The method of Claim 7, wherein said second tier biometric sensor (104, 106) is a comparatively more sophisticated biometric sensor than said first tier biometric sensor (102).

9. A method for selectively activating biometric sensors (102, 104, 106) to authenticate the identity of an individual while conserving system resources, comprising the acts of:

during an enrollment stage, enrolling said individual with a biometric system using first tier (102) and second tier biometric sensors (104, 106);

determining which first (102) and second tier biometric sensors (104, 106) result in a successful biometric verification of said individual thereby yielding enrollment biometric data for said individual;

storing the enrollment biometric data and a personal identification number (PIN) for said individual on a magnetic storage medium of a token;

during an operational stage, verifying the biometric of said individual comprising the acts of:

verifying the PIN stored on said individual's token;

using the enrollment biometric data stored on said token to activate only those first (102) and second tier biometric sensors (104, 106) which have been previously determined to result in said successful biometric verification of said individual during said enrollment stage; and

attempting to verify the biometric of said individual using only the activated biometric sensors.

10. The method of claim 9, wherein the token comprises a magnetic stripe having multiple tracks for storing the biometric enrollment data and PIN.

11. The method according to claim 9, wherein the token comprises at least one of an access card, credit card, debit card, identification card and smart card.

12. The method according to claim 9, wherein verifying the PIN comprises: reading the PIN from the magnetic storage medium; requesting a verification PIN from said individual; and comparing the PIN read from the magnetic storage medium with the verification PIN.

13. A system (100) for selectively activating biometric sensors (102, 104, 106) to authenticate the identity of an individual while conserving system resources, the system comprising:

a biometric security device (101) comprising a plurality of biometric devices;

at least one processor (107) connected to said biometric security device (101), said at least one processor (107) including one or more databases (108) for storing biometric and user data;

said processor (107) programmed to:

activate a first tier biometric sensor (102) to verify the biometric of said individual; and

activate a second tier biometric sensor (104, 106) to verify the biometric of said individual in the case where said individual is successfully verified with said first tier biometric sensor (102).

14. The system (100) of Claim 13, wherein said second tier biometric sensor (104, 106) is a comparatively more sophisticated sensor than said first tier biometric sensor (102).

15. A system (100) for selectively activating biometric sensors (102, 104, 106) to authenticate the identity of an individual while conserving system resources, the system (100) comprising:

a biometric security device (101) comprising a plurality of biometric devices;

at least one processor (107) connected to said biometric security device (101), said at least one processor (107) including one or more databases (108) for storing biometric and user data;

said processor (107) programmed to:

activate a first tier biometric sensor (102) to verify the biometric of said individual; and

activate a second tier biometric sensor (104, 106) to verify the biometric of said individual in the case where said individual is unsuccessfully verified with said first tier biometric sensor (102).

16. The system (100) of Claim 15, wherein said second tier biometric sensor (104, 106) is a comparatively more sophisticated sensor than said first tier biometric sensor (102).

17. A system (100) for selectively activating biometric sensors (102, 104, 106) to authenticate the identity of an individual while conserving system resources, the system (100) comprising:

a biometric security device (101) comprising a plurality of biometric devices;

at least one processor (107) connected to said biometric security device (101), said at least one processor (107) including one or more databases (108) for storing biometric and user data;

said processor (107) programmed to:

activate a first tier biometric sensor (102) to verify the biometric of said individual;

determining whether said individual desires a service level exceeding a predetermined service level threshold; and

activate a second tier biometric sensor (104, 106) to verify the biometric of said individual when it determined that said individual desires said service level exceeding said threshold.

18. The system (100) of Claim 17, wherein said second tier biometric sensor (104, 106) is a comparatively more sophisticated sensor than said first tier biometric sensor.

19. A system (100) for selectively activating biometric sensors (102, 104, 106) to authenticate the identity of an individual while conserving system resources, the system (100) comprising:

a biometric security device (101) comprising a plurality of biometric devices;

at least one processor (107) connected to said biometric security device (101), said at least one processor (107) including one or more databases (108) for storing biometric and user data;

said processor (107) programmed to:

activate a first tier biometric sensor (102) to verify the biometric of said individual;

determining whether an environmental parameter is outside of a predetermined range; and

activate a second tier biometric sensor (104, 106) to verify the biometric of said individual when said environmental parameter is determined to be outside said predetermined range.

20. The system (100) of Claim 19, wherein said second tier biometric sensor (104, 106) is a comparatively more sophisticated sensor than said first tier biometric sensor (102).

21. A system (100) for selectively activating biometric sensors (102, 104, 106) to authenticate the identity of an individual while conserving system resources, the system (100) comprising:

a biometric security device (101) comprising a plurality of biometric devices;

at least one processor (107) connected to said biometric security device (101), said at least one processor (107) including one or more databases (108) for storing biometric and user data;

said processor (107) programmed to:

during an enrollment stage, enrolling said individual with a biometric system using first tier (102) and second tier biometric sensors (104, 106);

determining which first (102) and second tier (104, 106) biometric sensors result in a successful biometric verification of said individual thereby yielding enrollment biometric data for said individual;

storing the enrollment biometric data and a personal identification number (PIN) for said individual on a magnetic storage medium of a token;

during an operational stage, verifying the biometric of said individual comprising the acts of:

verifying the PIN stored on said individual's token;

using the enrollment biometric data stored on said token to activate only those first (102) and second tier biometric sensors (104, 106) which have been previously determined to result in said successful biometric verification of said individual during said enrollment stage; and

attempting to verify the biometric of said individual using only the activated biometric sensors.

22. The system (100) of Claim 21, wherein said second tier biometric sensor (104, 106) is a comparatively more sophisticated sensor than said first tier biometric sensor (102).